SYSTEM AND METHODS FOR CONTACTLESS BIOMETRICS-BASED IDENTIFICATION

CROSS REFERENCE TO RELATED PATENTS

This application claims the benefit of U.S. Provisional Patent Application No. 61/936,685 filed Feb. 6, 2014, which is incorporated by reference.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH

This invention was made with government support under S51000000012539 awarded by the U.S. Department of Justice. The government has certain rights in the invention.

FIELD OF THE INVENTION

The present invention relates generally to a system and methods that facilitates the identification of an individual through the use of data. Certain more particular embodiments of the present invention facilitate the contactless acquisition and processing of biometric data for identification purposes. Certain preferred embodiments of the present invention of the system include apparatus by which the capture of one or more images of an individual may be facilitated for further processing. Advantageously, certain embodiments of the present invention facilitate the enrollment of one or more individuals for verification and identification purposes through the use of the data developed from the one or more captured images.

BACKGROUND OF THE INVENTION

A variety of systems and methods have been developed by which individuals may be identified so as, for example, to determine whether an individual may be permitted access or use a service or apparatus.

One traditional means of identification uses a token, such as a social security card, driver's license, passport, or key card, by which an individual may be identified. In such case, each individual that seeks to be identified through the use of the token must complete the necessary steps first to acquire the token. The completion of these steps may take a large amount of time. For example, it is well known that a person seeking to acquire a passport must obtain, fill out, and submit an application, then wait days and possibly weeks for the application to be reviewed and the analog passport dispatched to the person. The person must carry the analog passport in order to be able to use the passport as a means of identification. Many such token-based identification systems are based on at least a first assumption that whoever has possession of the token is actually the person identified by the token. Since certain lost or stolen tokens can provide, for example, access to unauthorized individuals, individuals using such tokens for identification purposes must take additional steps to maintain possession of the token at all times. To prevent unauthorized use, tokens often include additional complex features to help verify that the person having possession of the token is, in fact, the person authorized to have or identified by the token.

Another traditional means of identification is based on the use of information that is intended to be unique to each individual. Examples of information that are used for such knowledge-based identification systems include charge card numbers, social security numbers, passwords, mother's maiden names, and personal identification numbers ("PIN"). A person with knowledge of the information can, for example, gain access to a service or the use of an apparatus. However, as with token-based identification systems, knowledge-based identification systems can be misused. The information can be improperly obtained and used.

Another means of identification uses biometric identifiers. Biometric identifiers are based on the physical characteristics of individuals that can be measured or quantified. Conventional biometric identifiers use either the physiological characteristics or the behavioral characteristics of individuals. The physiological characteristics of individuals that can be used to develop biometric identifiers can be obtained from a variety of biometric sources including fingerprints, palm prints, face recognition, DNA, and retina or iris recognition. Behavioral characteristics that can be used as biometric identifiers include the typing rhythm, the gait, and the voice of individuals.

One or more disadvantages are associated with most conventional biometric-based identification systems. For example, behavioral characteristics—such as individual gait or voice patterns—are not inherently unique to one individual and may be imitated. While a physiological characteristic—such as a finger print, the retinal characteristics, or the DNA of an individual—does provide a unique identifier, the conventional systems and methods that are used to generate such biometric identifiers typically require the expenditure of considerable time, money, and other resources to develop the information and, in the case of a DNA-based biometric system, can raise a variety of privacy concerns. Also, many conventional systems that require an individual to match the stored biometric identifier in order, for example, to lock or unlock an apparatus or obtain a service have various shortcomings associated with them. To illustrate this point, the acquisition and use of a certain biometric identifier—fingerprints—for purposes of locking and unlocking cellular telephones will now be discussed.

Cellular telephones are one of the most widely used technological devices on the planet. Cellular telephones are used not only to place and receive phone calls, but also communicate through other messaging, plus as digital still and video cameras, music and video players, and lightweight computers. Given all these uses, individuals have come to acquire and retain some of their most private information on cellular telephones.

To prevent unauthorized access to this private information, and overall the use of misappropriated cell phones, a variety of systems have been developed. One common system permits an owner to select a password that must be entered into the phone before any further access or use is permitted. However, in order to gain quick access to and be able to use the phone, most people choose a password that is short in length and easy to remember. The security of such a phone is easily compromised. To improve the security of the phones, some phone systems allow an individual to use the information obtained from a scan of a fingerprint or other body part as the basis for a password. The 15 million bits of information contained within a fingerprint can provide the basis for a password that is far more secure than the typical short combination of letters and numbers chosen by the public.

To obtain the information from a body part, such as a fingerprint, that can be used as the basis for a system password, typically an image of the body part must be captured. Some conventional systems for acquiring fingerprint images rely on the physical contact between the soft tissue of the examined finger and a scanning element.